

We claim:

1. A method for controlling access to a media file, the method comprising:

generating a first authorization ticket at a first time in response to a request to access the media file from a user;

generating a second authorization ticket at a second time;

determining whether the first and the second authorization tickets match thereby determining whether the user is authorized to access the media file;

generating a first hash at a third time, the first hash based upon the determining whether the authorization tickets match and upon data;

generating a second hash at a fourth time, the second hash based upon the data;

determining whether the first hash and the second hash match, wherein a match of the first and second hashes indicates the user as having been authorized; and

permitting the user access to the media file if the first and second hashes match.
2. The method of claim 1 wherein the permitting access includes permitting access to multiple media files.
3. The method of claim 1 wherein the first and the second authorization tickets do not match, thereby indicating attempted unauthorized access and wherein the first hash has a value that indicates that access is to be denied.
4. The method of claim 1 wherein a first server generates the first hash and a second server permits the user access, the first server being different than the second server.
5. The method of claim 1 wherein a first server determines whether the first and second authorization tickets match, and a second server permits the user access, the first server being different than the second server.
6. The method of claim 1 wherein:
the first authorization ticket is generated on a web server;

the second authorization ticket is generated and the determination whether the first and the second authorization tickets match are performed on a global cache server;

the first hash is generated on a playlist server; and

the generating of the second hash, the determining whether the first hash and the second hash match, and the permitting the user access to the media file are all performed on a media server.
7. The method of claim 1 wherein the request is received from a user's computer and wherein the data is a cookie on the user's computer.

8. The method of claim 1 wherein the data is a randomly generated string.
9. The method of claim 1 wherein the data is a null value.
10. The method of claim 1 wherein the data is a date.
11. The method of claim 10 wherein the date is a future date.
12. The method of claim 10 wherein the date is the present date.
13. The method of claim 10 wherein the date is a past date.
14. The method of claim 1 further comprising:
 - generating a third authorization ticket at the second time; and
 - comparing the first authorization ticket to each of the second and the third authorization tickets.
15. The method of claim 1 wherein the first authorization ticket and the second authorization ticket are based on a time.
16. The method of claim 15 wherein the time is a future time.
17. The method of claim 15 wherein the time is the present time.
18. The method of claim 15 wherein the time is a past time.
19. The method of claim 1 wherein the first authorization ticket and the second authorization ticket are based on a security key.
20. The method of claim 1 wherein the first authorization ticket and the second authorization ticket are based on an identifier for the media file.
21. The method of claim 1 wherein the first hash and the second hash are further based on a time.
22. The method of claim 21 wherein the time is a future time.
23. The method of claim 21 wherein the time is the present time.
24. The method of claim 21 wherein the time is a past time.
25. The method of claim 1 wherein the first hash and the second hash are further based on a security key.
26. The method of claim 1 wherein the first hash and the second hash are further based on an identifier for the media file.
27. A system for controlling access to a media file, the system comprising one or more processors operative with software to:
 - generate a first authorization ticket at a first time in response to a request to access the

media file;

generate a second authorization ticket at a second time independently of the first authorization ticket and to determine whether to grant access to the media file by comparing the first authorization ticket and the second authorization ticket;

generate a first hash based upon the determination of the second processor; and

generate a second hash;

determine whether to grant access to the media file by comparing the first hash and the second hash; and

provide access to the media file, based on the comparing of the first hash and the second hash.

28. The system of claim 27 wherein the controlling access is controlling access to multiple media files.

29. The system of claim 27 further comprising a web server, global cache server having local memory, playlist server and media server wherein:

the web server generates a first authorization ticket at a first time in response to a request to access the media file;

the global cache server generates a second authorization ticket at a second time independently of the first authorization ticket and determines whether to grant access to the media file by comparing the first authorization ticket and the second authorization ticket;

the playlist server generates a first hash based upon the determination of the second processor; and

the media server determines whether to grant access to the media file by comparing the first hash and the second hash and provides access to the media file, based on the comparing of the first hash and the second hash.

30. A method for controlling access to a media file, the method comprising:

receiving a request from a first user, the first user having first user data associated therewith;

generating a first authorization ticket based upon the first user data;

generating a second authorization ticket based upon the first user data;

determining that the first authorization ticket matches the second authorization ticket, thereby indicating that the first user is authorized;

generating a first hash based upon the determining of the authorization tickets and the first user request;

receiving a request from a second user, the second user having second user data associated therewith;

in response to the second user request, generating a second hash;

determining that the first hash and the second hash do not match, thereby indicating the second user has not been authorized; and

denying the second user access to the media file.

31. The method of claim 30 further comprising:

in response to the first user request, generating a third hash based upon the comparison of the first authorization ticket and the second authorization ticket

determining the first hash matches the third hash, thereby indicating that the first user has been authorized; and

granting the first user access to the media file.

32. The method of claim 30 wherein the controlling access is controlling access to multiple media files.

33. The method of claim 30 wherein the third data is the fourth data.

34. A computer readable medium comprising computer code for instructing one or more processors to:

receive a first authorization ticket generated in response to a request to access a media file;

generate a second authorization ticket independently of the first authorization ticket;

compare the first authorization ticket and the second authorization ticket;

generate a first hash based upon the comparing of the authorization tickets and data; and

transmit the first hash.